EXHIBIT 2

I. INTRODUCTION

I, Dennis Nathan Cain, declare under penalty of perjury the foregoing is true and correct to the best of my knowledge and belief. I am an adult of sound mind residing in Berkley County, West Virginia. I make this declaration of my own free will and accord without coercion and with no mental reservation.

I have been retained as an expert witness on behalf of Petitioners in the above captioned proceeding. I expect to testify on the following subject matters: (i) application of the federal law's requirements for certification of the voting systems used in the November 3rd, 2020 general election, (ii) render opinions that based on available government records, news stories, photographic and video evidence, affidavits by first hand witnesses, reports by experts in data analysis, cybersecurity, and election operations, that voting systems were noncompliant with said law and therefore not certified, (iii) and render opinions that the vote tally and everything thereafter was therefore "void ab initio".

This is a statement of my relevant opinions and an outline of the factual basis for these opinions. The opinions and facts contained herein are based on the information made available to me in this case prior to preparation of this report, as well as my professional experience as a cybersecurity information systems security professional and expert in government IT systems certification and accreditation.

I reserve the right to supplement or amend this statement on the basis of further information obtained prior to the time of trial or in order to clarify or correct the information contained herein.

II. QUALIFICATIONS

I am a Cybersecurity Subject Matter Expert with a combined 23 years' experience in information assurance, risk management, vulnerability assessment, systems engineering, and systems certification assessment and authorization. I currently maintain and have held a TOP SECRET clearance with a Single Scope Background Investigation (SSBI) for 22 years. I hold credentials as a Certified Information Systems Security Professional (CISSP) #420251 since April 30, 2012 and

as Navy Qualified Validator (NQV) and have worked for Army, Navy, Marine Corps, DISA, FBI, and others.

I first began serving my country as a US ARMY soldier, where I was trained as a Telecommunications Computer Oper/Maint 74G at US Army Signal School in Fort Gordon GA in 1997. I then served as a Department of the NAVY civilian Information Technology Specialist IT-2210-GS-13 (INFOSEC) where I was the Information Systems Security Officer (ISSO) for my command. Finally, I served as US Marine civilian, where I was trained in NSA's CYBERCORE program at PHNX II and appointed as a member of a MARFORCYBER Cyber Protection Team (CPT) National Mission, whose core responsibility was protecting national critical infrastructure against cyber-attack by domestic and foreign adversaries. In all three of these times of service I swore an oath that I would "…support and defend the Constitution of the United States against all enemies, foreign and domestic; that I will bear true faith and allegiance to the same…".

As a former FBI whistleblower, where I had nothing to gain and under threat of reprisal, I am the only person to have brought a complaint of urgent concern on a matter of National Security to the IG of the Department of Justice, Michael Horowitz. I believe this testifies to my integrity as a witness and commitment to the oath I swore three times.

I am currently employed with cleared defense contractor Assett, Inc as a Senior Cybersecurity Engineer and provide systems cybersecurity assessment as a NQV for US NAVY, NAVSEA, TSUBCYBER for their Submarine program. My work consists of consulting as a Subject Matter Expert trusted agent, validating Navy information and weapon systems for compliance with NIST Special Publication 800 series, specifically the NIST SP 800-53rev4 Security Controls and various ISO standards.

These same standards are cited as requirements for certification of all electronic voting systems under both Help America Vote Act (HAVA) under the Federal Election Commission (FEC) Voting Systems Standards (VSS), Volume I and the Federal Information Security Modernization Act (FISMA).

I was brought together with a team of experts in various fields related to election operations, process, and cybersecurity, due to my expertise and knowledge of government IT systems cybersecurity certification requirements, during which time in the months on November 2020 and December 2020, I volunteered approximately 435 hours of my time this work to the non-partisan Thomas More Society – Amistad Project and other legal efforts to ensure our election integrity. The bulk of my work consisted of reviewing the laws and regulations related to voting systems certification evidence of irregularities of the November 3rd, 2020 general election. I also consulted on non-compliance issues being discovered during subsequent investigations to these various legal group and provided expert witness testimony.

III. DOCUMENTS & EVIDENCE REVIEWED

During my period of consultation, I reviewed the following items that applied to the voting systems used in the November 3rd general election. They consisted of:

A. Legislation

- Help America Vote Act, Pub. L. 107-252, 42 USC Sections 15301-15545
- Civil Rights Act of 1960, Retention and preservation of records and papers by officers of elections, 42 USC 1974
- Voting Rights Act of 1965, Pub. L. 89-110, 42 USC Sections 1973; 1973a-p; 1973aa; 1973aa-1-6; 1973bb; 1973bb-1
- Federal Information Security Management Act of 2002, Pub. L. 107-347,
- Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 et seq., Public Law (P.L.) 113-283.
- Various State Election Laws

B. Policies & Standards

- Office of Management and Budget [OMB] Circular A-130 "Managing Information as a Strategic Resource"
- Federal Election Commission (FEC) Voting Systems Standards, Volume 1 2002
- National Institutes of Standards & Technology (NIST) Special Publication (SP) 800 Series on Computer Security
- EAC State Requirements and the U.S. Election Assistance Commission Voting System Testing and Certification Program, September 4, 2020

C. Guidelines & Manuals

- Election Assistance Commission (EAC) Voluntary Voting Systems Guidelines, Volume 1 & 2, Version 1.1

- Defense Information Systems Agency (DISA) Security Technical Implementation Guides
- Cybersecurity & Infrastructure Security Agency (CISA) Election Security Checklists and Guides
- EAC Voting System Testing and Certification Program Manual, Version 2.0, May 31, 2015

D. Evidence Sources

- AMISTAD PROJECT 2020 evidence page– a release of evidence of voter, ballot, and election irregularities and lawlessness in the presidential election of November 3, 2020 <https://got-freedom.org/evidence/>
- HERE IS THE EVIDENCE website – a crowdsourcing tool for organizing anomalies and legal issues surrounding the irregularity of this current 2020 Presidential Election (news reports, photo evidence, video evidence, affidavits, expert analysis, etc.) <https://hereistheevidence.com/>
- Antrim Michigan Forensics Report – Revised Preliminary Summary, v2 dated 12/13/2020 and produced by Allied Security Operations Group (ASOG). <https://www.9and10news.com/content/uploads/2020/12/Antrim_Michigan_Forensics_Report_121320_v2_REDACTED.pdf>
- Electionware Admin Audit Event Logs & Election Audit Logs Events reports from Williamson County, TX Generated on 11/16/2020 <https://kmpuag.bn.files.1drv.com/y4m3byaJlYark6VJFnE_6oxwSb-hTacstnJ6KamqGMYshqqr7nSjlZZcPX-PGxocxp6QdxUyAg1jdCGuutQKaImnj9IYShKyJylLYHeJLGZk1bNY22EqrA6ez8GEr0CixOaiCajTctYL-KEkjKcSKL1jx6WF1Ysgs3HfMfVBsT-GxLbsSlG4TytZJ2aONSNVc9Zrt_HtK78TJFowjAUjC087g>

IV. COMPENSATION

I have been retained as an expert witness for Petitioners. I am not being compensated.

V. PRIOR TESTIMONY

I have not provided testimony as an expert either at trial or in deposition in the last four years.

VI. STATEMENTS OF OPINIONS

A. Violations of HAVA, Section 301 Voting Systems Standards and FISMA

As set forth above, I have been engaged to provide expert opinions regarding analysis in the November 3, 2020 general election. Based on my review of the documents set forth above, my discussions with statisticians and analysts working with me and at my direction, my discussions with the attorneys representing the Petitioners, I have the following opinions:

Certification plays an integral role in ensuring the integrity of the election. Once a system is certified it is authorized to process voting information and count the votes. Without certification a system cannot be trusted and therefore everything processed on it is void. One of the primary purposes of the certification process is to confirm in a laboratory setting that the voting system meets the maximum allowable error rate under the law. This rate is set at a sufficiently stringent level such that the likelihood of voting system errors affecting the outcome of an election is exceptionally remote even in the closest of elections. A failure to meet the acceptable maximum rate of error is "void ab initio".

An example that many will understand is in the case of a DWI being tried before the court. In such a case the arresting officer is required to demonstrate that his equipment used to validate the defendants blood alcohol level (breathalyzer) has been certified to be calibrated to within an acceptable error rate as to not accidentally falsely convict an innocent person. Therefor if the system is found to not be certified or be out of compliance with certification requirements, then all evidence produced be the equipment must be thrown out as it is "void ab initio" or void from the beginning. So is the case where the error rate exceeds the maximum allowable error rate in any part of the voting system as it could disenfranchise the constitutional rights of the citizens of the United States.

I conducted a review of the Electionware Election Audit Logs Events report from Williamson County, TX Generated on 11/16/2020. The event log registered several hundred errors that may indicate a more serious problems with ES&S voting machines that were used in Texas. According to the Table of Voting Systems found on the EAC's Systems Certification Process website <https://www.eac.gov/voting-equipment/system-certification-process> the system used in Williamson county is a EVS, version 6.0.2.0, manufactured by ES&S and is certified by EAC. The certificate of conformity can be found at:

<https://www.eac.gov/sites/default/files/voting_system/files/EVS6020_CertConf_Scope%28FINAL%29.pdf>

A significant finding was an error event "The file is no longer available", which occurred 808 times consecutively on 11/03/2020 from 09:03:08PM to 09:03:13PM. This indicates an anomaly that should have prompted the local election official to submit an Anomaly Report to the

EAC and a request for a fielded system review and testing to be conducted IAW EAC Voting System Testing and Certification Program Manual, Version 2.0, section 8.7. "An anomaly is defined as an irregular or inconsistent action or response from the voting system, or system component, which resulted in the system or component not functioning as intended or expected. reviews will be conducted to ensure that a fielded system is comprised of the same configuration as what was certified by the EAC and that the proper Mark of Certification has been applied. As this system is approved for use in 149 counties across the United States, this is particularly concerning as is could indicate a greater problem affecting multiple states. Further examination of the audit logs and batches processed during that period of time should be conducted to ensure that this anomaly is not indicative of a more wide-spread problem.

A review of the Antrim Michigan Forensics Report – Revised Preliminary Summary, v2 dated 12/13/2020 and produced by Allied Security Operations Group (ASOG) indicated an error rate finding that would invalidate the certification of the voting system (Dominion Voting Systems Suite 5.5). On page 3, Item 10 it presents that "in Central Lake Township there were 1,222 ballots reversed out of 1,491 total ballots cast". This vote flip constitutes a total of 2,444 ballot position errors if you are only counting the Presidential race. A sample of the ballot for Central Lake Township 2020 General election indicates a total of 94 total ballot positions available to select from. Multiplied by the total number of ballots cast it equals a total of 140,154 ballot positions for the total vote count in that precinct. This calculated error rate for the system by the FEC VSS section 3.2.1 formula is 1.74% when the maximum allowable error rate is only .0002%. That is a rate of error that exceeds 8,718 times the acceptable rate of error.

Formulas:

1. *2,444 (total ballot position errors)/140,154 (total ballot positions cast) = .017437961099329 (error rate)*
2. *.017437961099329(error rate)/.000002 (maximum allowable error rate) = 8,718.98 (X allowable rate)*

The allowable error rate for the Dominion Voting System Suite 5.5 as certified by EAC has been exceeded at such a high rate with multiple reports of similar errors in Oakland County MI (Heart Civic Voting System) and Wayne County MI (Dominion Voting System), Spalding County Georgia (Dominion Voting Systems), Philadelphia County, PA (ES&S Voting Systems)

that it clearly indicates a systemic problem with either the certification process or the Baseline, Promotion, and Demotion Procedures identified in the FEC VSS Vol.1 Sections 8.4. This failure to comply invalidates all confidence in the integrity of the vote count under the Help America Vote Act (HAVA).

Compliance with the Federal Information Security Modernization Act (FISMA) is also required of electronic voting systems. On January 6th, 2017, DHS Secretary Jeh Johnson designated election infrastructure as a critical infrastructure subsector:

<https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical.>

This effectively placed all election equipment under the requirements set forth by the Federal Information Security Modernization Act (FISMA) of 2014 (PL 113-283, 44 USC 3554). The Cybersecurity Framework, when used in conjunction with NIST's 800-37 Rev 2 Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, 800-39, Managing Information Security Risk: Organization, Mission, and Information System View and associated standards, guidelines, and best practices provides agencies with a comprehensive structure for making more informed, risk-based decisions and managing cybersecurity risks across their enterprise.

The primary standards used for identifying Security Control risks is the NIST SP 800 53rev4. This document details the standard configuration settings, policies, and procedures for security compliance with all government information systems in conjunction with FIPS – 199 the Standard for systems categorization. The items identified in the ASOG report on page 15, section I, paragraph 2 items a) through i) and several news reports, affidavits, videos, and pictures indicate several violations with the requirements set forth in the above-mentioned standards:

- A fairly complete list of these irregularities listed by state has been detailed in the following article: <https://sharylattkisson.com/2020/11/what-youve-been-asking-for-a-fairly-complete-list-of-some-of-the-most-significant-claims-of-2020-election-miscounts-errors-or-fraud/>

- A website dedicated to making public all of the available evidence of irregularity in the 2020 general election has identified, as of the time of the writing of this declaration, has identified 1,570,056 ballots touched by anomalies, 920 fact

witnesses, and 34+courts that have blocked evidentiary hearings. <https://hereistheevidence.com/election-2020/stats/>

- A release of evidence of voter, ballot, and election irregularities and lawlessness in the presidential election of November 3, 2020 by the Amistad Project <https://got-freedom.org/evidence/>

These violations indicate potential misconfigurations, changes to the secure baseline, failure to comply with procedures and policies, negligence, or malfeasance. Failure to comply with said standards in any normal situation under the Risk Management Framework would invoke action by the approving authority to revoke the information systems certification through a process called "Decertification". HAVA requires that the EAC certify and decertify voting systems. Section 231(a)(1) of HAVA specifically requires the EAC to "* * * provide for the testing, certification, decertification and recertification of voting system hardware and software by accredited laboratories." The Procedural Manual for the Election Assistance Commission's Voting System Testing and Certification Program describes "Decertification" in section 1.5.1.6 as "the process by which the EAC revokes a certification it previously granted to a voting system. It is an important part of the Certification Program because it serves to ensure that the requirements of the program are followed and that certified voting systems fielded for use in Federal elections maintain the same level of quality as those presented for testing."

These systems are required to undergo an annual audit under FISMA requirements to assess the cybersecurity situational awareness of the information system. There is no indication by the reported non-compliance with NIST SP 800-53rev4 that the systems are following the annual audit requirements under the law. Additionally, the HAVA, FEC VSS, and the Election Assistance Commission (EAC) Voluntary Voting Systems Standard (VVSS) all point to the NIST SP 800-53rev4 as the standard for Security Controls compliance. The current state of electronic voting systems in many states do not appear to meet with the standards, This should prompt a full compliance audit with both the FEC VSS (2002), NIST SP 800 37rev2 Risk Management Framework, and NIST SP 800-53rev4 Security Controls for all of electronic voting systems where irregularities have been identified. If, during the audit, it is determined that these systems no longer meet "the level of quality as those presented for testing" then under the law of both HAVA and FISMA these systems are not authorized for processing votes. This would in effect invalidate all

certification of the votes where these uncertified machines where used as it would render impossible any attempt to validate the integrity of the vote count performed electronically.

B. Violations of Civil Rights Act of 1960, Section 1974

All auditing capability is dependent of the retention of auditable items to include all paper, electronic media, and digital logs associated with an election. There have been multiple news report, affidavits, physical evidence found, video footage, and photographs taken of evidence of the destruction of such auditable items.

The law clearly states under §1974. Retention and preservation of records and papers by officers of elections; deposit with custodian; penalty for violation, "Every officer of election shall retain and preserve, for a period of twenty-two months from the date of any general, special, or primary election of which candidates for the office of President, Vice President, presidential elector, Member of the Senate, Member of the House of Representatives, or Resident Commissioner from the Commonwealth of Puerto Rico are voted for, all records and papers which come into his possession relating to any application, registration, payment of poll tax, or other act requisite to voting in such election, except that, when required by law, such records and papers may be delivered to another officer of election and except that, if a State or the Commonwealth of Puerto Rico designates a custodian to retain and preserve these records and papers at a specified place, then such records and papers may be deposited with such custodian, and the duty to retain and preserve any record or paper so deposited shall devolve upon such custodian. Any officer of election or custodian who willfully fails to comply with this section shall be fined not more than $1,000 or imprisoned not more than one year, or both." (Pub. L. 86–449, title III, §301, May 6, 1960, 74 Stat. 88 .)

Failure to comply with retention and preservation of records and papers by officers of elections does not adequately allow for any meaningful audit. The voting system certified under the authority of the EAC includes more then just the electronic voting machine. It includes all component identified in the certificate of conformity held by the EAC and includes an accreditation boundary and everything within it to include everything coming in and going out related to the election (i.e. ballots, registration logs, poll books, security envelopes, outer envelopes, chain of

custody logs, digital logs, software enumeration reports, accounts enumeration reports, memory cards, hard drive storage, voting machine logic chips, etc.) All of these types of auditable items are required to be maintained unmolested and secured for 22 months.

VII. REQUEST FOR FURTHER INFORMATION

As set forth above, I have been engaged to provide expert opinions regarding analysis in the November 3, 2020 general election. Based on my review of the documents set forth above, my discussions with statisticians and analysts working with me and at my direction, my discussions with the attorneys representing the Petitioners, I request the following additional information for assisting me in my investigation.

1. Documents regarding mobile drop boxes. Logs maintained regarding the drop boxes including, but not limited to, when drop box ballots were collected and delivered, the log of persons who collected drop boxes or delivered ballots from drop boxes and who had access to drop box keys and when that access was obtained.

2. Documents or logs maintained on the delivery of ballots to central counting facilities used in major metropolitan areas including the identity of each and every person involved in delivering the ballots.

3. Documents or logs maintained identifying the persons who tabulated the ballots are any central counting facility including, but not limited to, logs of who was tabulating ballots and at what time.

4. Documents maintained regarding each and every local official involved in handling ballots and how those individuals were paid. As you know, a lawsuit has been filed asserting that an organization called the Center for Technology and Civic Life (CTCL), Center for Election Innovation and Research (CEIR), and Electronic Registration Information Center (ERIC), organizations funded by FaceBook billionaire Mark Zuckerberg, who paid millions of dollars to pay the salaries of local officials to count the votes.

5. The pollbooks, voter files and final tallies at each election site in large cities over 250,000 people.

6. Documents regarding challenged ballots including how many ballots were challenged, how many challenged ballots were cast and why such ballots were cast despite being challenged.

7. Documents regarding why republicans were not allowed to sign the seals at the polling places both prior to voting on Monday and on Wednesday before ballot boxes were documented, closed, and locked

8. Documents showing that information placed was directly into the Qualified Voter Files in the AVCBs.

9. Documents showing how many voter birthdates were altered in the pollbooks.

10. Documents showing how many ballots were counted at central counting which were not reflected in the electronic pollbook or paper supplemental list.

11. Documents showing the verifications of the same day registrations in on November 3 including the verifications used to verify that these persons could vote.

12. Documents regarding "Rock the Vote" including, but not limited to, why this highly partisan organization was given access in real time through data feeds, internet hookups and API access to voters' private information including their social security numbers, birthdays, drivers licenses numbers, address, and eye color.

13. Documents related to persons who did not vote in the county in which they resided, voted and then moved out of the State or voted in more than one state.

14. Documents regarding ballots cast with the names of citizens who did not do the voting.

15. Documents regarding ballots cast by individuals who are deceased.

16. Documents regarding ballots cast by felons or the criminally insane.

17. Documents regarding election officials who either ignored or refused to record valid election challenges.

18. Documents regarding the back dating of absentee ballots.

19. Documents regarding sending multiple absentee ballots to the same address.

20. Documents regarding credentialed challengers being locked out of the vote counting rooms.

21. Documents regarding duplication of ballots.

22. Documents regarding election workers who encouraged or coerced voters to vote in a certain manner.

23. Documents regarding those counties that had more registered voters than citizens of legal voting age.

24. Documents regarding the disregard of voter secrecy or use of privacy sleeves.

25. Documents regarding the different treatment applied to military or veterans ballots.

26. Documents regarding ballots received after the statutory deadline.

27. Documents regarding people added to the voters rolls (QVF) after the statutory deadline.

28. Documents regarding tabulator computers connected to the internet including why this was allowed and how it was conducted.

29. Documents regarding adjudicator computers connected to the internet including why this was allowed and how it was conducted.

30. Documents regarding the use of counting board computers hosting the electronic poll books connected to the internet including why this was allowed and how it was conducted.

31. Documents regarding "stage" computers used by Election Officials connected to the internet including why this was allowed and how it was conducted.

32. Documents identifying all Wi-Fi networks used at central counting locations.

33. Documents regarding the hacking of computers used in the election process.

34. Documents regarding how vote tallies were reported to both to the State and the media.

35. Documents regarding how many ballots/AVCBs were processed through paper pollbooks, electronic pollbooks including those processed through QVF.

36. Documents regarding where and when ballots were processed through the QVF including now this was verified and whether poll challengers were allowed and able to observe this process.

37. Documents regarding any investigation into why AVCBs which tallied zero ballots, yet the corresponding lock boxes had ballots inside the lock box.

38. Each and every chain of custody log for each lock box containing ballots.

39. Documents regarding how chain of custody was kept for ballots between worker shift changes.

40. Documents regarding which lock boxes were locked between shift changes

41. Documents regarding why any lock boxes left open during shift changes.

42. Documents regarding the process when the ballot's number didn't match the pollbook.

43. Documents regarding ballot stub numbers which were manually altered in the electronic pollbooks to match the ballot number on the paper ballot received including what would happen if the original ballot was later received.

44. Documents regarding how many ballot stub numbers were manually changed in pollbooks.

45. Documents regarding under what circumstances would it be appropriate to alter voter birthdates including how many birthdates were altered and how many voter QVF's showed voters who were born in the year 1900 or earlier.

46. Documents regarding the residents registered for same-day registration including how these ballots were processed and verified against a pollbook.

47. Documents regarding the use of an "unrestricted list" including why it was used and how it was used and the list itself.

48. Documents regarding absentee ballots requested but never returned.

49. Documents regarding what happened to unsolicited absentee ballots that were sent but never returned.

50. Documents regarding private funding of the election including, but not limited to, CTCL money and "walking around" money used near polling places.

51. Stored memory of the official vote count and ballot images for audit trail in the DRE machines.

52. Digital audit records generated for each component of the electronic voting system.

53. All Windows event logs (System, Application, Security, Setup, etc.) for each component of the electronic voting system.

54. A copy of the Windows System wide registry and all individual User Registry files for each component of the electronic voting system.

55. A list of all User Accounts for each component of the electronic voting system.

56. Full directory listing of all files with metadata for each component of the electronic voting system.

57. A full credentialed Nessus vulnerability scan for every component of the electronic voting system along with the mandated vulnerability scan performed as part of the approved and certified baseline for each component of the electronic voting system.

58. A list of all software, versions, and dates of installation for each component of the electronic voting system.

59. A WLAN report (netsh wlan show) for each component of the electronic voting system.

I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct. Executed on January 18, 2021.

/s/ Dennis Nathan Cain

Dennis Nathan Cain